

ISO/IEC TR 24729-4:2009-03 (E)

Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: Tag data security

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and abbreviated terms	2
5	Background	2
5.1	System definition: tag, tag to reader, reader	2
5.2	Definition of security	3
5.3	Security objectives	3
6	RFID data access security risk assessment	4
6.1	Risk assessment	4
6.2	Probability	5
7	Threats	6
7.1	Skimming data	6
7.2	"Eavesdropping" or "sniffing" on transmission between tag and reader	7
7.3	Spoofing	7
7.4	Cloning	7
7.5	Data tampering	7
7.6	Malicious code	7
7.7	Denial of access/service	7
7.8	Unauthorized killing the tag (electronic or mechanical)	7
7.9	Jamming/Shielding	7
8	Scenarios	8
8.1	Unsecured access control card, no personal identification number (PIN); No encryption or other security feature	8
8.2	Secured access control card, no PIN; Encrypted or other security features	8
8.3	Customer Loyalty Card	9
8.4	EPC Label (Batch Tag ID only)	9
8.5	Contactless Payment, No PIN	10
8.6	Contactless Payment, PIN	10
8.7	Contactless Payment, Biometric or other physical activation	10
8.8	Pharmaceutical e-Pedigree	11
8.9	Example of Impact	11
8.10	Summary	12
9	Types of security safeguarding countermeasures	13
9.1	Wafer programming (true WORM)	14
9.2	ISO Tag ID verification	14
9.3	License plate	14
9.4	Memory lock	14
9.5	Password protection	14

9.6	Authentication	14
9.7	Cloaking/Data security (obfuscated ID)	15
9.8	Encryption	15
9.9	Limitation of read distance	15
9.10	Summary	16
10	Threat response "best practices"	16
	Annex A (informative) Encryption	17
	Bibliography	20